Web Security:

Content Counts

Linda Brown

Office of the Assistant Secretary of Defense
(Command, Control, Communications & Intelligence)

DoD Web Policy

"Using the World Wide Web is strongly encouraged in that it provides the DoD with a powerful tool to convey information quickly and efficiently on a broad range of topics relating to its activities, objectives, policies and programs."

Web Site Administration Policies and Procedures, Part I, para 4.1

DoD Web Policy

"The considerable mission benefits gained by using the Web must be carefully balanced through the application of comprehensive risk management procedures against the potential risk to DoD interests, ... created by having electronically aggregated DoD information more readily accessible to a worldwide audience."

Web Site Administration Policies and Procedures, Part I, para 4.2

The Dilemma

How to balance mission benefits against potential risks

The Dilemma Restated

"It is the policy of the Department of Defense to make available timely and accurate information so that the public, Congress, and the news media may assess and understand the facts about national security and defense strategy."

- Secretary Cohen, 1 Apr 97

The Dilemma Restated

"I am amazed at the amount and content of open-source material available over the Internet from US military and other government agencies... An enemy of the US does not need to have specific war/operations plans when so much info about US doctrine is openly available."

Precursors

- Initial web policy issued 1995
  - Public Affairs focus
- Eligible Receiver ‘97
- Solar Sunrise
- Recognition of growing dependence and growing vulnerabilities
  - Availability of personal information on military members and families

DoD Web Site Administration Policy & Procedures

- Issued by DepSecDef, Dec 98
- Policy and procedures for establishing, operating, maintaining unclassified web sites, including those run by contractors
- Assigns management responsibility to Heads of Components
- Specifies OPSEC process and provides guide for identifying data “inappropriate” for posting

What is OPSEC?

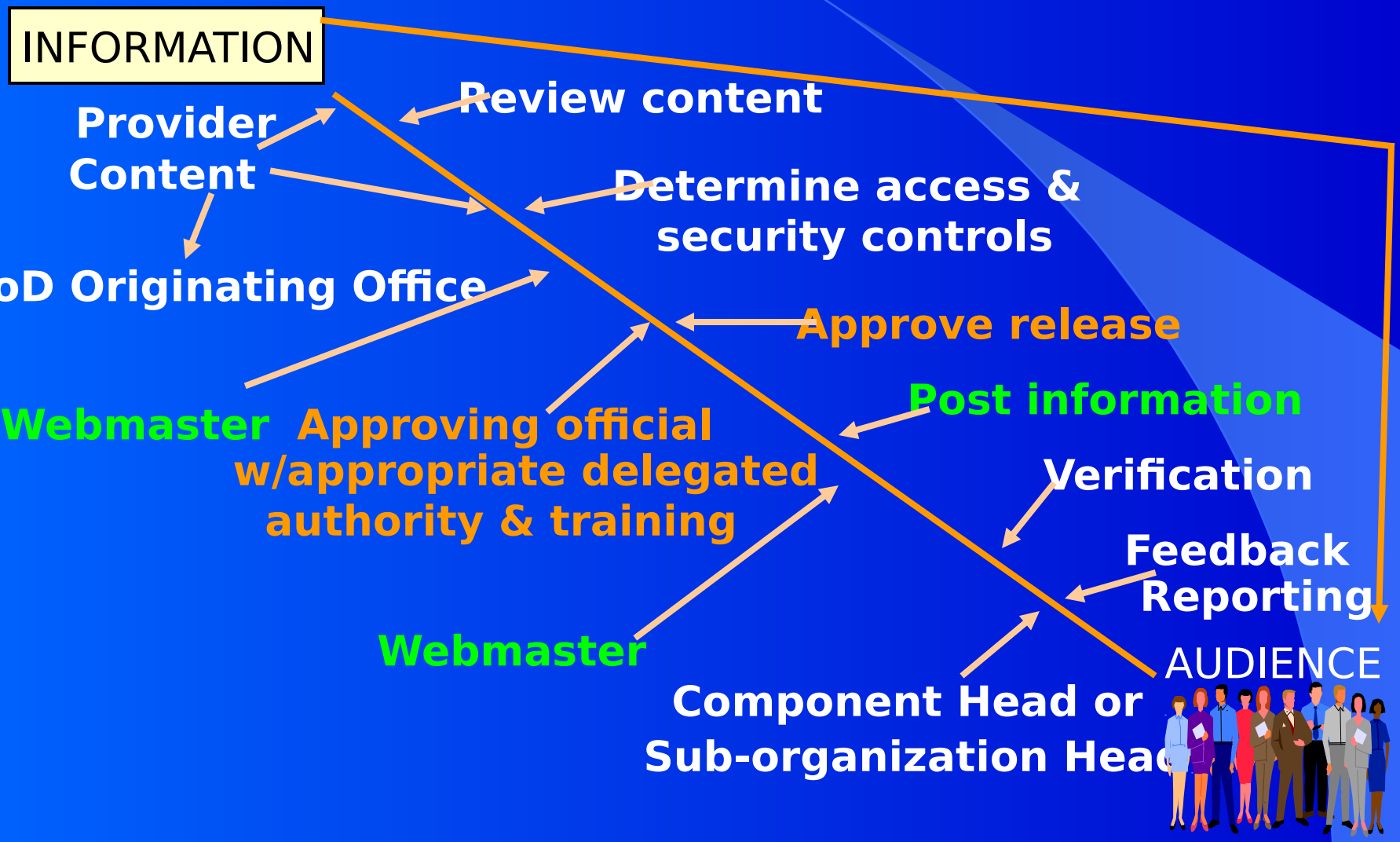
- Analytic process
- Value of unclassified information
- Focus on adversaries

OPSEC Methodology

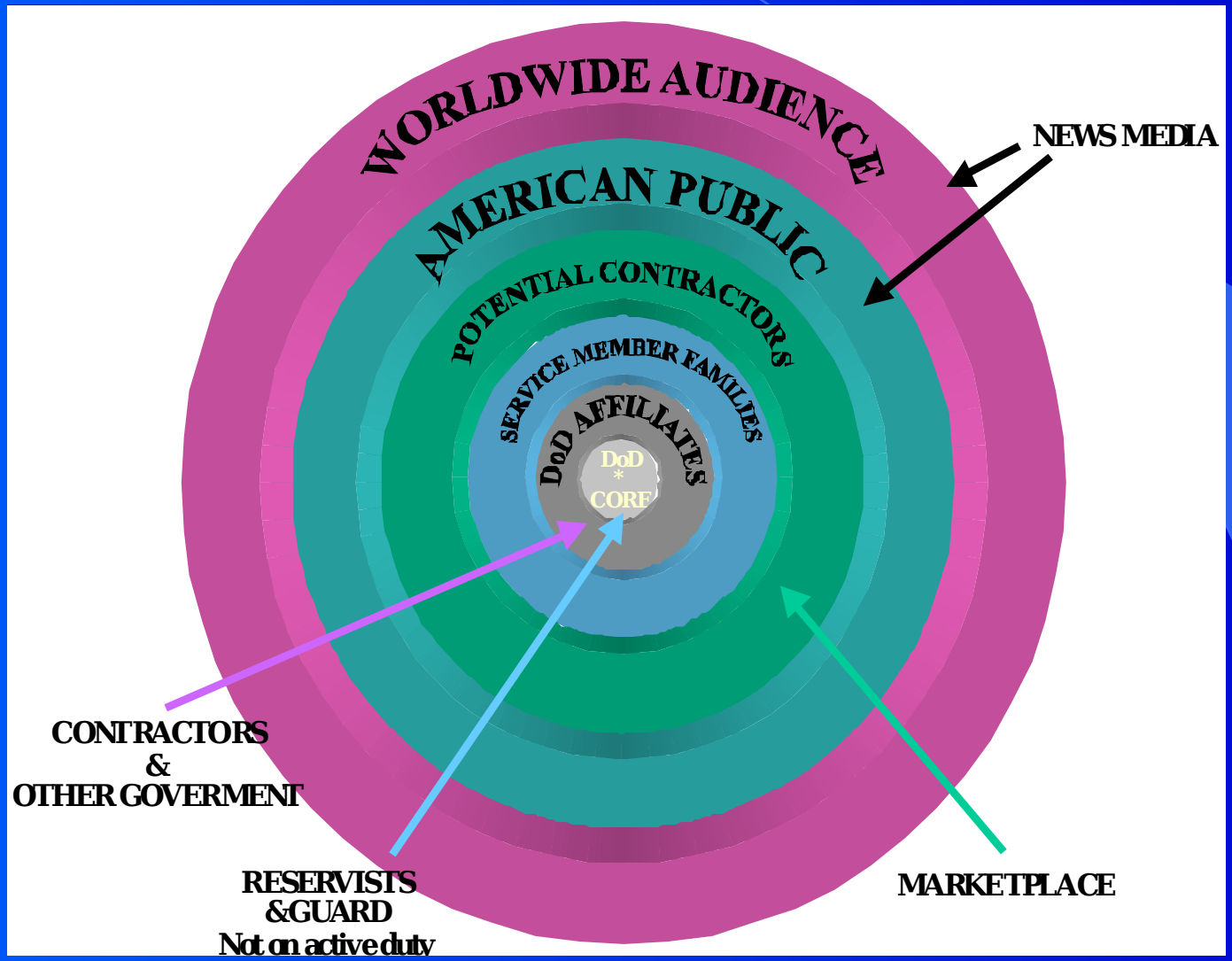
National **S**ecurity **D**ecision **D**irective **298**

- Analyze Threat
- Identify Critical Information
- Analyze Vulnerabilities
- Assess Risk
- Apply Countermeasures

Information Posting Process

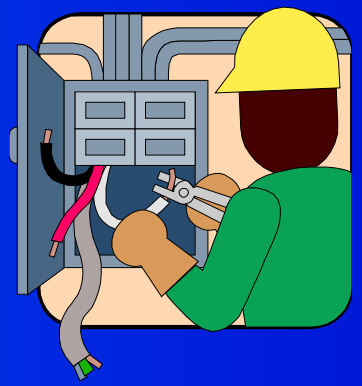


Audience


WORLDWIDE AUDIENCE
AMERICAN PUBLIC
POTENTIAL CONTRACTORS
SERVICE MEMBER FAMILIES
DoD AFFILIATES
DoD
*
CORE
NEWS MEDIA
CONTRACTORS
&
OTHER GOVERMENT
RESERVISTS
&GUARD
Not on active duty
MARKETPLACE

Audience or Adversary?

- Enemies
- Competitors
- Employees
- Terrorists
- Criminals
- News Media



The Threat

- An adversary can use any computer, at any location, at any time to collect information, without alarming the target installation or program or its security personnel to this type of surveillance
- No special skills, other than patience, required

Critical Information

What do you need to protect to be successful?

What must you keep from your adversary to be successful?

Vulnerability Issues

- Size/scope of DoD web presence (~200 GB; every domain; rapid turnover)
- Understanding of “publicly accessible”
- Identifying “inappropriate information”
- Aggregation of data
  - How much is too much?
  - How to identify?

“Publicly Accessible”

A web site available worldwide

without access controlled via an authentication mechanism

(user id / password or PKI certificates)

that precludes general access

“Publicly Accessible”

- Sites utilizing domain (e.g., .mil.,gov) or IP address restrictions without additional access controls are considered publicly accessible
- Posted information must be unclassified, non-sensitive, and cleared/authorized for public release

Examples of "Inappropriate Information"

- Personal/Privacy Act information
  - SSN, date of birth, home address, phone numbers (except appropriate duty phone numbers)
  - Names, address, identifying information about family members
- Detailed org charts and phone directories
- Plans or lessons learned which reveal sensitive operations, exercises, or vulnerabilities
- Sensitive scientific and technical information
- Detailed installation data

Current Sites

Army CONUS Installation

- Maps of installation with location of facilities
- Phone directory with direct numbers
- Details of base utilities and critical infrastructure nodes
  - Distribution maps for water, power, natural gas systems
- Photos of installation
- Hospital staff bios containing names of family members

Source: Duncan Van Buskirk,

Current Sites

DOD OCONUS Installation

PMO INTERNAL PHONE DIRECTORY
MP DESK: xxxxxxx, ADMIN xxxxxxx
Civilian numbers are prefix xxxxxxxxxxxx

Section:	Contact:	Phone:
Provost Marshal	LTC ----------	xxxxxxxxx
Provost Sergeant	MSG ----------	xxxxxxxxxx
Operations Officer	----------	xxxxxxxxx
Police Liaison	----------	xxxxxxxxx
IMO	----------	xxxxxxxxx
Desk Sergeant	----------	xxxxxxxxx
Alarms Monitor		xxxxxxxxx
Physical Security	SGT ----------	xxxxxxxxx
Military Police Inv.	MPI ----------	xxxxxxxxx
	MPI ----------	xxxxxxxxx
Mil. Working Dogs	SSG ----------	xxxxxxxxx
	SGT ----------	xxxxxxxxx
Pass & ID	----------	xxxxxxxxx
CID	----------	xxxxxxxxx
Em.Action C. EAC	SSG ----------	xxxxxxxxx

Note – All personnel information has been removed, as well as email addresses which were also included in the

D. Van Buskirk,

Compliance

Joint Web Risk Assessment Cell (JWRAC)

- Formation directed by DepSecDef
  - CONOPS approved Feb 99
  - Began operations in April 99
- Focus is OPSEC of public Web content
  - Policy compliance and data aggregation
- DISA is Executive Agent
- Staff = 2 Active Duty, 20 Reservists

Web Site Compliance: Some Significant Findings

- One classified document; FOUO information
- Mission Area Plans, including mission needs / operational requirements data(MNS/ORD)
- Detailed personal/organizational data
  - Org charts (some with photos) -- Home phone
  - Bios with family info, exact DOB -- SSN
- CONOPS and SOPs
- Briefings/budget data intended for select audiences
- Detailed exercise info, lessons learned

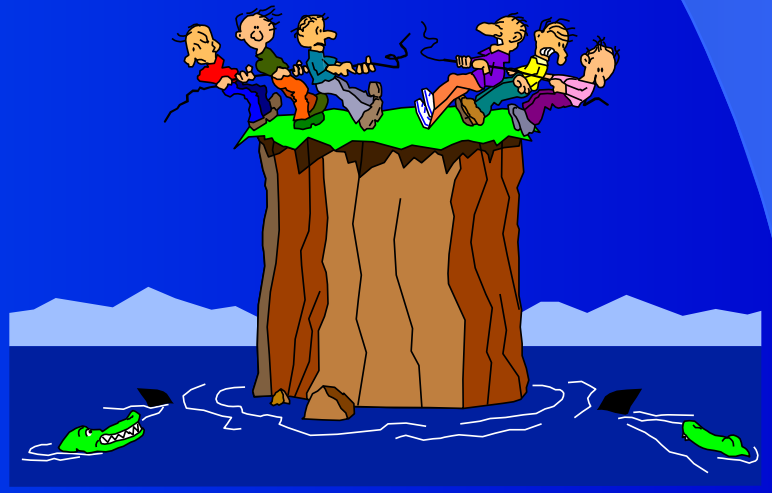
Problem Areas

- Inadequate monitoring and risk assessment of postings
- Inconsistent (or lack of) OPSEC training and awareness
- Personnel unfamiliar with policy
  - Its existence and requirements
  - Their responsibilities

Recent Issues

FOIA and the Web

- If it's releasable, why shouldn't it be posted?
  - Push & Pull
  - Need-to-know



FirstGov

- Federal web portal/search site
  - www.firstgov.gov
- Purpose: to make US government information more readily accessible to the public
- Technically two parts:
  - Front-end = user interface
  - Back-end = search system

FirstGov

- Indexes sites for keyword searches
  - Index built using spiders on .mil/.gov sites
  - Soon to index files in other formats (e.g., .doc, .ppt, .xls, .pdf)
- Impact of indexing other file formats?
  - Level of compliance with policy unknown
  - Eliminates “security by obscurity”

Privacy & Accessibility

- Privacy/use of “cookies”
  - Cookies can be used to track individual usage/persons
  - “Session” cookies / “persistent” cookies
- Section 508 compliance (access for persons with disabilities)
  - Final standards issued December 21, 2000
  - Compliance required June 21, 2001
  - FAR amendment currently being worked

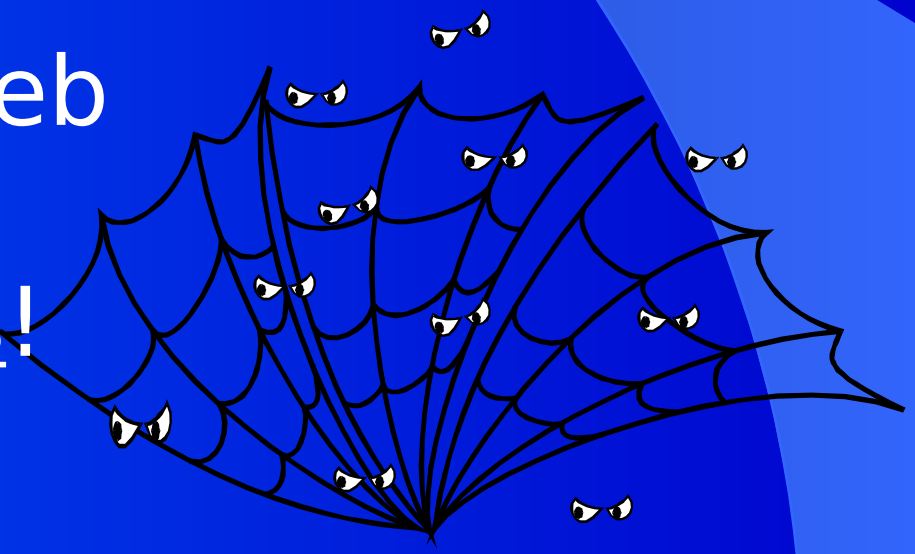
“Snapshot”

- On Jan 12, NARA requested “snapshot” of all publicly-accessible Federal web sites on/before Jan 20
- Problems for DoD
  - Suspense date
  - Cost/effort for the **150 GB** “snapshot”
  - Technical submission requirements
- Alternative close to agreement

Bottom Line

Content Counts!

- Generally, no requirement to have a web site
  - FOIA sites required
- If you have a web site/presence, content counts!



Solution is Simplicity

- Ask yourself:
  - What is the need for this information to be resident on the Web, and is this level of detail required?
  - Who is the audience for this information, and do security and access controls appropriately limit access?
  - Can the information be used to adversely impact operations or personnel?

Questions?

"… the information that turns the tide in a conflict is not always something locked up in a safe, or obtained from traditional espionage methods, but rather it can be information derived from open, unclassified sources available to anyone who knows where to look."
-- Lt. Gen Michael V. Hayden,
DIRNSA

References and Contact

- DoD Home Page:
  http://www.DefenseLINK.mil
- DoD Web Site Administration Policy:
  http://www.DefenseLINK.mil/admin/dod_web_policy_12071998.html
- Point of Contact:
  Linda D. Brown
  OASD(C3I)/Security Directorate
  (703) 695-2289 DSN 225-2289
  Linda.Brown@osd.mil